UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,973	12/04/2003	Thomas A. Crispin	CNTR.2071	7683

23669 7590 09/10/2007
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
HA, LEYNNA A	
ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
09/10/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	**Application No.** 10/727,973	**Applicant(s)** CRISPIN ET AL.	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-29,31-35 and 37-57* is/are pending in the application.

4a) Of the above claim(s) *10,30 and 36* is/are ~~withdrawn from consideration~~ Cancelled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-29,31-35 and 37-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *5/2/07;5/31/07;6/22/07*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9, 11-29, 31-35, and 37-57 are pending.

Claims 10, 30, and 36 have been cancelled by applicant.

2. The objection for claims 47-49 is withdrawn.

Response to Arguments

3. Applicant's arguments with respect to claims 1-9, 11-29, 31-35, and 37-39 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9, 11-29, 31-35, and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hashimoto, et al. (US 6,983,374), and further in view of Muratani, et al. (US 7,194,090).

Claim 1:

Hashimoto discloses an apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, be executed on a plurality of input text blocks; and **(col.10, lines 37-60 and col.28, lines 34-42)**

execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, wherein said one of the cryptographic operations, wherein said execution logic comprises: **(col.5, lines 58-67 and col.10, lines 5-8)**

a cryptography unit, *[configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit]*, and wherein said plurality of input text blocks are retrieved from memory, and wherein said plurality of output text blocks are stored to said memory; **(col.11, lines 60-65)**

indicating whether said one of the cryptographic operations has been interrupted by an interrupting event. **(col.6, lines 1-18 and col.12, lines 52-55 and col.13, lines 16-20;** Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col.9, lines 38-40 and col.27, lines 29-31). Thus, Hashimoto reads on the claimed interrupting event.)

Hashimoto discloses a cryptography unit but did not further include a plurality of cryptographic rounds.

Murantani discloses an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption (col.3, lines 19-23). Murantani discloses the round function as the claimed cryptographic rounds where the common key encryption system employing expanded keys in a reversed order between for encryption and for decryption (col.7, lines 10-17). Murantani discloses this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (col.9, lines 38-51 and col.10, lines 20-32).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Hashimoto with Murantani teaching cryptographic rounds or round functions because this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (Murantani – col.9, lines 38-51 and col.10, lines 20-32).

Claim 2: see Hashimoto on col.10, lines 8-10 and 37-41; discussing an apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises: an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

Claim 3: see col.5, lines 64-67 and col.11, lines 54-65; discussing an apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises: a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

Claim 4: see Hashimoto on col.10, lines 55-64; discussing the apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

Claim 5: see Hashimoto on col.11, lines 13-16; discussing the apparatus as recited in claim 1, wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations.

Claim 6: see Hashimoto on col.3, lines 13-16; discussing the apparatus as recited in claim 5, wherein said block cipher mode comprises electronic code book (ECB) mode.

Claim 7: see Hashimoto on col.18, lines 17-18; discussing the apparatus as recited in claim 5, wherein said block cipher mode comprises cipher block chaining (CBC) mode.

Claim 8: see Hashimoto on col.18, lines 17-18; discussing the apparatus as recited in claim 5, wherein said block cipher mode comprises cipher feedback mode (CFB) mode.

Claim 9: see Hashimoto on col.5, lines 49-50; discussing the apparatus as recited in claim 5, wherein said block cipher mode comprises output feedback (OFB) mode.

Claim 10: Cancelled.

Claim 11: see Hashimoto on col.6, lines 1-18 and col.7, lines 1-3 and col.12, lines 52-55; discussing the apparatus as recited in claim 10, further comprising: a bit, coupled to said execution logic, configured to indicate whether said one of the cryptographic operations has been interrupted by said interrupting event.

Claim 12: see Hashimoto on col.22, lines 48-50 and col.26, lines 58-60; discussing the apparatus as recited in claim 11, wherein said bit is contained within a flags register.

Claim 13: see Hashimoto on col.27, lines 59-62; discussing the apparatus as recited in claim 12, wherein said flags register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

Claim 14: see Hashimoto on col.12, lines 52-55; discussing the apparatus as recited in claim 1, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input data block is interrupted.

Claim 15: see Hashimoto on col.23, lines 59-60; discussing the apparatus as recited in claim 14, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input data block.

Claim 16: see Hashimoto on col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify pointers to input and output data blocks in said memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block.

Claim 17: see Hashimoto on col:21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

Claim 18: see Hashimoto on col.6, lines 1-18 and col.7, lines 1-3 and col.12, lines 52-55; discussing the apparatus as recited in claim 1, further comprising: block pointer logic, operatively coupled to said execution logic, configured to direct said computing device to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

Claim 19: see Hashimoto on col.9, lines 51-52 and col.12, lines 60-63; discussing the apparatus as recited in claim 1, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

Claim 20: see Hashimoto on col.3, lines 1-2 and col.11, lines 54-63; discussing the apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

Claim 21: see Hashimoto on col.3, lines 33-34 and col.11, lines 13-28; discussing the apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

Claim 22: see Hashimoto on col.11, lines 13-28 and col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in said memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

Claim 23: see Hashimoto on col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of said plurality of output text blocks, said plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

Claim 24: see Hashimoto on col.3, lines 33-34 and col.27, lines 58-60; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

Claim 25: see Hashimoto on col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in said memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

Claim 26: see Hashimoto on col.5, lines 8-11; discussing the apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key.

Claim 27: see Hashimoto on col.5, lines 60-62; discussing the apparatus as recited in claim 25, wherein said cryptographic key data comprises a cryptographic key schedule.

Claim 28: see Hashimoto on col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in said memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

Claim 29: see Hashimoto on col.21, lines 30-32 and col.27, lines 31-33; discussing the apparatus as recited in claim 21, wherein said plurality of registers comprises: a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth-location in said memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

Claim 30: see Hashimoto on col.6, lines 1-2 and 37-40; discussing the apparatus as recited in claim 1, wherein said execution logic comprises: a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

Claim 31:

Hashimoto discloses the apparatus for performing cryptographic operations, comprising:

a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic **(col.10, lines 37-60 and col.28, lines 34-42)** operations, and wherein said cryptography unit *[is configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output data blocks]*, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of output data blocks are retrieved from memory; and **(col.11, lines 60-65)**

block pointer logic, operatively coupled to said cryptography unit, configured to direct said devices to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input datablocks; and **(col.11, lines 12-28 and col.13, lines 42-47)**

a bit within a register **(col.26, lines 58-60 and col.27, lines 59-62)**, operatively coupled to said cryptography unit, configured to indicate that execution of said one of the cryptographic operations has been interrupted by an interrupting event. **(col.6, lines 1-18 and col.12, lines 52-55 and col.13, lines 16-20;** Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col.9, lines 38-40 and col.27, lines 29-31). Thus, Hashimoto reads on the claimed interrupting event.)

Hashimoto discloses a cryptography unit but did not further include a plurality of cryptographic rounds.

Murantani discloses an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption (col.3, lines 19-23). Murantani discloses the round function as the claimed cryptographic rounds where the common key encryption system employing expanded keys in a reversed order between for encryption and for decryption (col.7, lines 10-17). Murantani discloses this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (col.9, lines 38-51 and col.10, lines 20-32).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Hashimoto with Murantani teaching cryptographic rounds or round functions because this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (Murantani – col.9, lines 38-51 and col.10, lines 20-32).

Claim 32: see Hashimoto on col.6, lines 1-18 and 61-63; discussing the apparatus as recited in claim 31, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

Claim 33: see Hashimoto on col.26, lines 58-60 and col.27, lines 58-60; discussing the apparatus as recited in claim 31, wherein said register comprises an EFLAGS register within an x86-compatible microprocessor, and wherein said bit comprises bit 30 within said EFLAGS register.

Claim 34: see Hashimoto on col.13, lines 16-20; discussing the apparatus as recited in claim 31, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input data block is interrupted.

Claim 35: see Hashimoto on col.6, lines 1-18 and col.12, lines 52-55; discussing the apparatus as recited in claim 34, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input data block.

Claim 36: cancelled

Claim 37: see Hashimoto on col.13, lines 42-45; discussing the apparatus as recited in claim 31, block pointer logic is configured to direct said device to modify contents of a block counter register to indicate that said one of the cryptographic operations has been completed on a current input data block.

Claim 38: see Hashimoto on col.13, lines 16-20 and 42-45; discussing the apparatus as recited in claim 31, wherein said block pointer logic is configured to direct said device to preserve or to generate and preserve data resulting from performance of said one of the cryptographic operations on a current block of data such that, upon return from said interrupting event, performance of said one of the cryptographic operations can continue with a following block of data.

Claim 39: see Hashimoto on col.3, lines 1-2; discussing the apparatus as recited in claim 31, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 40-57 are rejected under 35 U.S.C. 102(e) as being anticipate by Hashimoto, et al. (US 6,983,374).

Claim 40:

Hashimoto discloses method for performing cryptographic operations in a device, the method comprising:

retrieving a plurality of input data blocks from memory; **(col.11, lines 60-65)** executing one of the cryptographic operations on the plurality of input of data blocks to generate a corresponding plurality of output data blocks **(col.5, lines 58-67),** wherein said executing is performed responsive to receiving a cryptographic instruction, and wherein the cryptographic instruction prescribes the one of the cryptographic operations; **(col.10, lines 37-60 and col.28, lines 34-42)**

storing the corresponding plurality of output data blocks to the memory; and **(col.11, lines 24-26)** indicating whether an interrupting event has occurred during said executing. **(col.6, lines 1-18 and col.12, lines 52-55 and col.13, lines 16-20;** Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col.9, lines 38-40 and col.27, lines 29-31). Thus, Hashimoto reads on the claimed interrupting event.)

Claim 41: see col.11, lines 52-55 and col.13, lines 16-20; discussing the method as recited in claim 40, wherein said indicating comprises pointing out whether an interrupt, an exception, a page fault, or a task switch has occurred during said executing.

Claim 42: see col.26, lines 58-60 and col.27, lines 58-60; discussing the method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in a register within the device.

Claim 43: see col.26, lines 58-60 and col.27, lines 58-60; discussing the method as recited in claim 41, wherein said indicating comprises modifying the state of a bit in an EFLAGS register within an x86-compatible microprocessor.

Claim 44: see col.13, lines 16-20; discussing the method as recited in claim 40, further comprising: transferring program control to a program flow configured to process the interrupting event, and interrupting said executing of the one of the cryptographic operations on a current input data block.

Claim 45: see col.10, lines 32-64; discussing the method as recited in claim 44, further comprising: upon return of program control to said cryptographic instruction following said transferring, performing said executing on said current input data block.

Claim 46: see col.21, lines 30-32 and col.27, lines 31-33; discussing the method as recited in claim 40, further comprising: directing the device to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of the one of the cryptographic operations on a current input data block.

Claim 47: see col.26, lines 58-60 and col.27, lines 58-60; discussing the method as recited in claim 40, further comprising: directing the device to modify contents of a block counter register to indicate that the one of the cryptographic operations has been completed on a current input data block.

Claim 48: see col.10, lines 55-64; discussing the method as recited in claim 40, further comprising: directing the device to preserve or to generate and preserve data resulting from performance of the one of the cryptographic operations on a current block of data such that, upon return from the interrupting event, performance of the one of the cryptographic operations can continue with a following block of data.

Claim 49: see col.3, lines 1-3; discussing the method as recited in claim 40, wherein said receiving comprises: prescribing the cryptographic instruction according to the x86 instruction format.

Claim 50: see col.14, lines 60-61; discussing the method as recited in claim 40, wherein said receiving comprises: prescribing an encryption operation as the one of the cryptographic operations, wherein the encryption operation comprises encryption of the plurality of input data blocks to generate the corresponding plurality of output data blocks.

Claim 51: see col.14, lines 60-61 and col.17, lines 48-49; discussing the method as recited in claim 40, wherein said receiving comprises: prescribing a decryption operation as the one of the cryptographic operations, wherein the decryption operation comprises decryption of the plurality of input data blocks to generate the corresponding plurality of output data blocks.

Claim 52: see col.10, lines 55-64; discussing the method as recited in claim 40, wherein said executing comprises: accomplishing the one of the cryptographic operations according to the Advanced Encryption Standard (AES) algorithm.

Claim 53: see col.18, lines 17-18; discussing the method as recited in claim 40, wherein said receiving comprises: specifying, within the cryptographic instruction, a block cipher mode to be employed in accomplishing the one of the cryptographic operations.

Claim 54: see col.3, lines 13-16; discussing the 54method as recited in claim 53, wherein the block cipher mode comprises electronic code book (ECB) mode.

Claim 55: see col.18, lines 17-18; discussing the method as recited in claim 53, wherein the block cipher mode comprises cipher block chaining (CBC) mode.

Claim 56: see col.18, lines 17-18; discussing the method as recited in claim 53, wherein the block cipher mode comprises cipher feedback mode (CFB) mode.

Claim 57: see col.5, lines 49-50; discussing the method as recited in claim 53, wherein the block cipher mode comprises output feedback (OFB) mode.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

HOSUK SONG
PRIMARY EXAMINER